

CLAIMS

What is claimed is:

- 1 1. A computer implemented method comprising:
2 calling an operation from a first processor;
3 executing a plurality of primitive security operations at a second processor in
4 response to the operation call;
5 generating a set of data from executing the plurality of primitive security
6 operations; and
7 establishing a secure session with the set of data.
- 1 2. The computer implemented method of claim 1 wherein the set of data comprises:
2 a set of decrypted data;
3 a set of encrypted data; and
4 a set of hashed messages.
- 1 3. The computer implemented method of claim 2 further comprising a set of random
2 numbers.
- 1 4. The computer implemented method of claim 1 further comprising the first
2 processor calling a second operation to establish a second secure session.
- 1 5. The computer implemented method of claim 1 wherein the secure session is an
2 SSL 3.0 session, a TLS session, or an IPSec session.
- 1 6. A computer implemented method comprising:
2 calling a macro security operation;

3 performing a set of operations in response to the macro security operation, the set
 4 of operations comprising
 5 generating a secret and a key material,
 6 creating a first finished hash for a client message,
 7 creating a second finished hash for a server message,
 8 creating a finished message; and
 9 establishing a secure session.

1 7. The computer implemented method of claim 6 wherein the set of operations
 2 further comprises
 3 decrypting a pre-master secret; and
 4 decrypting a client finished message.

1 8. The computer implemented method of claim 6 wherein the set of operations
 2 further comprises generating a set of random numbers.

1 9. The computer implemented method of claim 6 wherein the set of operations
 2 further comprises creating an expected finished message.

1 10. The computer implemented method of claim 6 further comprising calling a second
 2 macro security operation to establish a second secure session.

1 11. A system comprising:
 2 a first network element to request a secure session; and
 3 a second network element networked to the first network element, the second
 4 network element to call a macro security operation from a first processor,
 5 to execute a plurality of primitive security operations at a second
 6 processor in response to the macro security operation cal and to generate a

7 set of data from the execution of the plurality of primitive security
8 operations.

1 12. The system of claim 11 wherein the set of data comprises:
2 a set of decrypted data;
3 a set of encrypted data; and
4 a set of hashed data.

1 13. The system of claim 11 wherein the first network element to request the secure
2 session comprises the first network element to transmit a set of messages to the second
3 network element, to execute a second macro security operation, and to generate a second
4 set of data from the execution of the second macro security operation.

1 14. The system of claim 11 further comprising a third network element networked to
2 the second network element, the third network element to request a second secure session
3 with the second network element.

1 15. The system of claim 11 further comprising:
2 the first network element to request a second secure session with the second
3 network element; and
4 the second network element to execute a second macro security operation to
5 establish the second secure session with the first network element.

1 16. An apparatus comprising:
2 a first processor to call a macro security operation to establish a secure session;
3 a second processor coupled to the first processor, the second processor to perform
4 a plurality of primitive security operations in response to the macro
5 security operation call; and

6 a memory coupled to the first and the second processor, the memory to store a set
7 of data generated by the second processor.

1 17. The apparatus of claim 16 wherein the second processor comprises:
2 a request unit to fetch and to distribute the macro security operation; and
3 a plurality of execution units coupled to the request unit, one of the plurality of
4 execution units to execute the plurality of primitive security operations.

1 18. The apparatus of claim 17 further comprising:
2 the first processor to call a second macro security operation after calling the first
3 macro security operation; and
4 a second one of the plurality of execution units to execute a second plurality of
5 primitive security operations corresponding to the second macro security
6 operation before the one of the plurality of execution units completes
7 execution of the plurality of primitive security operations.

1 19. The apparatus of claim 17 wherein the one of the plurality of execution units
2 comprises:
3 a microcode unit to translate the macro security operation into a plurality of
4 primitive security operations;
5 an execution queue unit coupled to the microcode unit, the execution queue unit to
6 queue the plurality of primitive security operations;
7 a plurality of primitive security operation units coupled to the execution queue
8 unit, the plurality of primitive security operation units to perform the
9 plurality of primitive security operations; and
10 a bus coupled to the plurality of primitive security operation units, the bus to
11 transmit data.

1 20. The apparatus of claim 16 further comprising the memory to store a set of source
2 data.

1 21. An apparatus comprising:
2 a first processor to call a macro security operation;
3 a second processor coupled to the first processor, the second processor comprising
4 a request unit to retrieve the macro security operation,
5 a plurality of execution units coupled to the request unit, one of the
6 plurality of execution units to perform a plurality of primitive
7 security operations, the plurality of primitive security operations
8 corresponding to the macro security operation; and
9 a memory coupled to the first and second processor, the memory to store a set of
10 data generated by the second processor.

1 22. The apparatus of claim 21 further comprising the memory to store a set of source
2 data from the host processor.

1 23. The apparatus of claim 21 wherein each of the plurality of execution units
2 comprises:
3 a microcode unit to translate the macro security operation into the plurality of
4 primitive security operations;
5 an execution queue unit coupled to the microcode unit, the execution queue unit to
6 queue the plurality of primitive security operations;
7 a plurality of primitive security operation units coupled to the execution queue
8 unit, the plurality of primitive security operation units to perform the
9 plurality of primitive security operations; and
10 a bus coupled to the plurality of primitive security operation units, the bus to
11 transmit the set of generated data.

10035509-131007

1 24. The apparatus of claim 21 further comprising:
2 the first processor to call a primitive security operation; and
3 a second one of the plurality of execution units to execute the primitive security
4 operations.

1 25. A machine-readable medium that provides instructions, which when executed by a
2 set of one or more processors, cause said set of processors to perform operations
3 comprising:
4 executing a macro security operation at a first one of the set of processors;
5 executing a plurality of primitive security operations at a second one of the set of
6 processors in response to the macro security operation call;
7 generating a set of data from executing the plurality of primitive security
8 operations; and
9 establishing a secure session with the set of data.

1 26. The machine-readable medium of claim 25 wherein the set of data comprises:
2 a set of decrypted data;
3 a set of encrypted data; and
4 a set of hashed messages.

1 27. The machine-readable medium of claim 26 wherein the set of data further
2 comprises a set of random numbers.

1 28. The machine-readable medium of claim 25 further comprising the first processor
2 calling a second operation to establish a second secure session.

1 29. The machine-readable medium of claim 25 wherein the secure session is an SSL
2 3.0 session, a TLS session, or an IPSec session.

1 30. A machine-readable medium that provides instructions, which when executed by a
2 set of one or more processors, cause said set of processors to perform operations
3 comprising:
4 calling a macro security operation from a first one of the set of processors;
5 performing a set of operations at a second one of the set of processors in response
6 to the macro security operation, the set of operations comprising
7 generating a secret and a key material,
8 creating a first finished hash for a client message,
9 creating a second finished hash for a server message,
10 creating a finished message; and
11 establishing a secure session.

1 31. The machine-readable medium of claim 30 wherein the set of operations further
2 comprises decrypting a pre-master secret and a client finished message.

1 32. The machine-readable medium of claim 30 wherein the set of operations further
2 comprises generating a set of random numbers.

1 33. The machine-readable medium of claim 30 the set of operations further
2 comprising creating an expected finished message.

1 34. The machine-readable medium of claim 30 further comprising calling a second
2 macro security operation to establish a second secure session.